CLAIM AMENDMENTS

1. (original) A device for generating an uncorrelated pseudo-random bit sequence uniformly distributed over a user-definable value K, where K+1 has m prime factors $q_1, q_2, ..., q_m$, comprising:

(a) an array of m-1 multipliers, where each multiplier is numbered in accordance to the multiplier's order in the array, where each multiplier has a first input for receiving a unique pseudo-random bit sequence, where each pseudo-random bit sequence r_i is uniformly distributed over a range (0,..., q_i-1), where i = 1, 2, ..., m, where each multiplier has additional inputs equal to the multiplier's order number for receiving as many of the m prime factors as possible starting with q_1, and where each of the multipliers has an output; and

(b) an array of m-1 adders, where each adder is numbered in accordance with the adder's order in the array; where each adder has a first input, a second input, and an output; where the first input of the first adder in the array receives a unique pseudo-random bit sequence, where the adders are connected in daisy-chain fashion so that the output of each adder is connected to the first input of the adder that immediately follows in the array, and where the second inputs of the adders are connected to the outputs multipliers that correspond in number within the respective arrays.

2. (original) The device of claim 1, wherein $q_1, q_2, ..., q_m$ are ordered from smallest value to largest value.

3. (original) A method of generating an uncorrelated pseudo-random bit sequence, comprising the steps of:

(a) selecting a user-definable value K, where K is a positive integer;

(b) factoring K+1 into m prime factors $q_1,q_2,...,q_m$;

(c) generating m pseudo-random sequences $r_1, r_2,..., r_m$, where each pseudo-random bit sequence r_i is uniformly distributed over a range (0,..., q_i-1), and where i = 1, 2, ..., m; and

(d) generating the uncorrelated pseudo-random sequence as

$$R = r_1 + q_1 r_2 + q_1 q_2 r_3 + ... + q_1 q_{2...} q_{m-1} r_m.$$

4. (original) The method of claim 3, wherein the step of factoring K+1 into m prime factors $q_1,q_2,...,q_m$, is comprised of factoring K+1 into m prime factors $q_1,q_2,...,q_m$, where $q_1,q_2,...,q_m$ are ordered from smallest value q_1 to largest value q_m.

5. (new) A device for generating in a cyrptographic system an uncorrelated pseudo-random bit sequence uniformly distributed over a user-definable value K, where K+1 has m prime factors $q_1,q_2,...,q_m$, comprising:

(a) an array of m-1 multipliers, where each multiplier is numbered in accordance to the multiplier's order in the array, where each multiplier has a first input for receiving a unique pseudo-random bit sequence, where each pseudo-random bit sequence r_i is uniformly distributed over a range (0,..., q_i-1), where i = 1, 2, ..., m, where each multiplier has additional inputs equal to the multiplier's order number for receiving as many of the m prime factors as possible starting with q_1, and where each of the multipliers has an output; and

(b) an array of m-1 adders, where each adder is numbered in accordance with the adder's order in the array; where each adder has a first input, a second input, and an output; where the first input of the first adder in the array receives a unique pseudo-random bit sequence, where the adders are connected in daisy-chain fashion so that the output of each adder is connected to the first input of the adder that immediately follows in the array, and where the second inputs of the adders are connected to the outputs multipliers that correspond in number within the respective arrays.

6. (new) The device of claim 5, wherein $q_1, q_2, \ldots, q_m$ are ordered from smallest value to largest value.